

# EQUIPMENT FOR ISSUING LICENSE, EQUIPMENT FOR REPRODUCING CONTENTS, METHOD FOR ISSUING LICENSE AND METHOD FOR REPRODUCING CONTENTS

**Publication number:** JP2002073421 (A)

**Publication date:** 2002-03-12

**Inventor(s):** AKASHI TERUO +

**Applicant(s):** MATSUSHITA ELECTRIC IND CO LTD +

**Classification:**

- international: G06F1/00; G06F12/14; G06F15/00; G06F21/00; G06F21/22; G06F21/24; G06Q30/00; G06Q50/00; H04L9/08; H04L9/32; G06F1/00; G06F12/14; G06F15/00; G06F21/00; G06F21/22; G06Q30/00; G06Q50/00; H04L9/08; H04L9/32; (IPC1-7): G06F1/00; G06F12/14; G06F15/00; G06F17/60; H04L9/08; H04L9/32

- European: G06F21/00N7D

**Application number:** JP20000262912 20000831

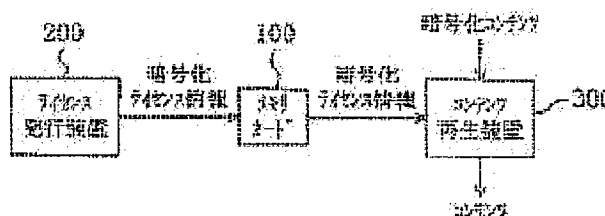
**Priority number(s):** JP20000262912 20000831

**Also published as:**

US2002026424 (A1)

## Abstract of JP 2002073421 (A)

**PROBLEM TO BE SOLVED:** To provide an equipment and a method by which user can uses contents without being limited by an equipment of play back. **SOLUTION:** An equipment for issuing license 200 encodes license information about contents which user wants, using an equipment ID of memory card 100 which user carries, and writes it into the memory card. An equipment for reproducing contents 300 decodes license information that is written into the memory card 100 which user carries, using an equipment ID of the memory card 100. And an equipment for reproducing contents 300 decodes contents that is decoded according to contents that is permitted to use license information that is decoded and reproduce it.



Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-73421

(P2002-73421A)

(43) 公開日 平成14年3月12日 (2002.3.12)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード <sup>*</sup> (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
			3 2 0 C 5 B 0 4 9
1/00		15/00	3 3 0 Z 5 B 0 7 6
15/00	3 3 0	17/60	1 4 2 5 B 0 8 5
17/60	1 4 2		3 0 2 E 5 J 1 0 4

審査請求 有 請求項の数19 O L (全 18 頁) 最終頁に続く

(21) 出願番号 特願2000-262912(P2000-262912)

(22) 出願日 平成12年8月31日 (2000.8.31)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 明石 輝夫

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100077931

弁理士 前田 弘 (外7名)

Fターム(参考) 5B017 AA03 BA05 BA07 CA14 CA16

5B049 AA05 GG06 GG10

5B076 FA05 FB06 FB11

5B085 AE13 AE23 AE29

5J104 AA07 AA12 AA16 EA03 KA02

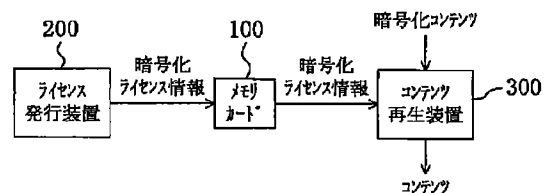
NA02 NA05 NA36 NA38 NA41

(54) 【発明の名称】 ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法

## (57) 【要約】

【課題】 再生装置に限定されずにコンテンツを利用できるようにする。

【解決手段】 ライセンス発行装置200は、利用者が希望するコンテンツのライセンス情報を、利用者が携帯するメモリカード100の装置IDを用いて暗号化して、当該メモリカード100に書き込む。コンテンツ再生装置300は、利用者が携帯するメモリカード100に書き込まれたライセンス情報を、当該メモリカード100の装置IDを用いて復号する。そして、コンテンツ再生装置300は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。



【特許請求の範囲】

【請求項1】 自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行装置であって、

利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、  
前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する手段と、

前記ライセンス情報作成手段によって作成されたライセンス情報を前記利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込む第1の暗号化手段とを備えることを特徴とするライセンス発行装置。

【請求項2】 請求項1に記載のライセンス発行装置において、  
前記ライセンス情報は、  
前記利用者によって指定されたコンテンツを識別するためのコンテンツIDを含むことを特徴とするライセンス発行装置。

【請求項3】 請求項1に記載のライセンス発行装置において、  
前記ライセンス情報は、  
前記利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むことを特徴とするライセンス発行装置。

【請求項4】 請求項1に記載のライセンス発行装置において、  
前記ライセンス情報は、  
前記利用者によって指定されたコンテンツを復号するための復号化鍵を含むことを特徴とするライセンス発行装置。

【請求項5】 請求項1に記載のライセンス発行装置において、  
前記認証手段は、  
前記利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、前記利用者が携帯するライセンス記憶装置の装置IDを暗号化する第2の暗号化手段を含み、  
前記第1の暗号化手段は、  
前記第2の暗号化手段によって暗号化された装置IDを用いて前記ライセンス情報を暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込むことを特徴とするライセンス発行装置。

【請求項6】 請求項1に記載のライセンス発行装置において、

前記ライセンス発行装置は、前記利用者が携帯するライセンス記憶装置にネットワークを介して接続されることを特徴とするライセンス発行装置。

【請求項7】 暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、  
前記コンテンツ再生装置は、

自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置IDを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、

前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置IDを用いて復号する復号手段と、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを備えることを特徴とするコンテンツ再生装置。

【請求項8】 請求項7に記載のコンテンツ再生装置において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含むものであり、

前記再生手段は、  
前記復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号することを特徴とするコンテンツ再生装置。

【請求項9】 請求項7に記載のコンテンツ再生装置において、  
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツIDを含むものであり、

前記再生手段は、  
前記復号手段によって得られたライセンス情報に含まれるコンテンツIDを用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得することを特徴とするコンテンツ再生装置。

【請求項10】 請求項7に記載のコンテンツ再生装置において、

前記コンテンツ再生装置はさらに、  
暗号化されたコンテンツを蓄積する手段を備え、

前記再生手段は、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを前記蓄積手段から取得することを特徴とするコンテンツ再生装置。

【請求項11】 請求項7に記載のコンテンツ再生装置において、

前記再生手段は、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得することを特徴とするコンテンツ再生装置。

【請求項12】 請求項7に記載のコンテンツ再生装置において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、

前記再生手段は、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生することを特徴とするコンテンツ再生装置。

【請求項13】 請求項12に記載のコンテンツ再生装置において、

前記コンテンツ再生装置はさらに、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生手段によるコンテンツの再生に応じて更新するコンテンツ利用条件更新手段と、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記コンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する手段と、

前記更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を前記利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化する手段と、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化手段によって暗号化された更新後ライセンス情報に書き換える手段とを備えることを特徴とするコンテンツ再生装置。

【請求項14】 暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、

前記コンテンツ再生装置は、

自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置ID、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいて

コンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置IDを暗号化して暗号化装置IDを生成する認証手段と、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記認証手段によって生成された暗号化装置IDを用いて復号する復号手段と、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを備えることを特徴とするコンテンツ再生装置。

【請求項15】 自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行方法であって、

利用者が携帯するライセンス記憶装置の正当性を認証し、

前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、

前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を前記利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込むことを特徴とするライセンス発行方法。

【請求項16】 暗号化されたコンテンツを復号して再生するコンテンツ再生方法であって、

前記コンテンツ再生方法は、

自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置IDを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証するステップと、

前記認証ステップにおいて前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置IDを用いて復号するステップと、

前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生するステップとを備えることを特徴とするコンテンツ再生方法。

【請求項17】 請求項16に記載のコンテンツ再生方法において、

前記再生ステップでは、

前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得することを特徴とするコンテンツ再生方法。

【請求項18】 請求項16に記載のコンテンツ再生方法において、  
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、  
前記再生ステップでは、  
前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生することを特徴とするコンテンツ再生方法。

【請求項19】 請求項18に記載のコンテンツ再生方法において、  
前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生ステップにおけるコンテンツの再生に応じて更新するステップと、  
前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、前記利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化するステップと、  
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化ステップによって暗号化された更新後ライセンス情報に書き換えるステップとをさらに備えることを特徴とするコンテンツ再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。さらに詳しくは、コンテンツと当該コンテンツのライセンスとを分離して提供するコンテンツ提供システムにおけるライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。

【0002】

【従来の技術】デジタル技術の発達により、ソフトウェアプログラムのみならず、絵画、音楽、映画などの著作物もデジタルデータとして管理され、流通するようになっている。近年ではさらに、ネットワーク技術の著しい進歩により、これらの著作物を、時間と場所を問わず、ネットワークを介して利用者に配布することが可能な環境が整いつつある。

【0003】デジタルデータとしてのこれらのコンテンツは、従来のアナログデータと異なり、複製を繰り返しても品質が劣化しない。したがって、コンテンツを販売

する側としては、流通しているコンテンツが著作権者の許可なく複製されるような不正利用を防止することが不可欠である。この点に関しては、暗号技術の発展がコンテンツのセキュリティレベルの向上に寄与している。暗号化技術としては、暗号化鍵と復号化鍵に同一の鍵を用いる対称暗号の一種であるDESや、暗号化と復号化とで鍵の異なる非対称暗号のRSA暗号などが知られている。

【0004】コンテンツの不正利用を防ぐ技術の第1の例として、販売しようとするコンテンツの全部または一部をあらかじめ暗号化してそのままでは利用不可能な状態に保護しておき、利用者が保護状態を解除するためのライセンスを購入する、という販売方式がある。この方式では、コンテンツを再生する装置に固有のIDを認識し、配布するライセンスをこのIDを含めて暗号化しておく。そして、再生時に、ライセンスを復号化して取り出したIDと再生装置に固有のIDとを比較して一致した場合にのみ再生を行う。このように、コンテンツを再生できる装置を限定し、不正に複製された装置上での利用を防いでいる。

【0005】また、第2の例として、ネットワーク上に管理センターを設け、コンテンツの再生時に、ネットワークを介して管理センターに接続し、パスワード等によりあらかじめ登録された利用者の認証を行うという手法がある。

【0006】

【発明が解決しようとする課題】上述の第1の例においては、コンテンツをライセンスとともに購入した後では、コンテンツを再生できる装置はライセンスを受けた再生装置に限定される。このため、コンテンツが自由に流通するようになって、そのコンテンツを利用するときには再生装置の制約を受ける。すなわち、特定のコンピュータにライセンスされたプログラムは、そのコンピュータにアクセスしなければ利用できない。家庭の据置型プレーヤにライセンスされた音楽は、外出先の携帯端末では利用できない。携帯型ビデオ再生装置にライセンスされた映画は、家庭内の大画面ディスプレイを備える装置では再生できない。このような種々の不具合が生じる。

【0007】また、上述の第2の例においては、ネットワークに接続でき、かつ管理センターと通信するための手段が不可欠となる。したがって、このような機能を持たない再生装置での利用は制限される。

【0008】

【課題を解決するための手段】この発明の1つの局面に従うと、ライセンス発行装置は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意的に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。ライセンス発行装置

は、認証手段と、ライセンス情報作成手段と、第1の暗号化手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。ライセンス情報作成手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する。第1の暗号化手段は、ライセンス情報作成手段によって作成されたライセンス情報を利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【0009】上記ライセンス発行装置では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0010】また、ライセンス情報は、ライセンス記憶装置の装置IDを用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0011】また、上記ライセンス発行装置は、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【0012】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【0013】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを識別するためのコンテンツIDを含む。

【0014】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。

【0015】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを復号するための復号化鍵を含む。

【0016】好ましくは、上記認証手段は、第2の暗号化手段を含む。第2の暗号化手段は、利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、利用者が携帯するライセンス記憶装置の装置IDを暗号化する。そして、上記第1の暗号化手段は、第2の暗号化手段によって暗号化された装置IDを用いてライセンス情報を

暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【0017】好ましくは、上記ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続される。

【0018】上記ライセンス発行装置によれば、利用者は、ライセンス発行装置と距離的に離れた所においても、ネットワークを介してライセンス発行装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【0019】この発明のもう1つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置IDを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。復号手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置IDを用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0020】上記コンテンツ再生装置では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0021】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0022】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコン

テンツを復号する。

【0023】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツIDを含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツIDを用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得する。

【0024】好ましくは、上記コンテンツ再生装置はさらに、蓄積手段を備える。蓄積手段は、暗号化されたコンテンツを蓄積する。そして、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを蓄積手段から取得する。

【0025】上記コンテンツ再生装置では、再生する可能性のあるコンテンツをあらかじめすべて蓄積手段に蓄積しておくことにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【0026】好ましくは、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【0027】上記コンテンツ再生装置では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0028】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0029】好ましくは、上記コンテンツ再生装置はさらに、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを備える。コンテンツ利用条件更新手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、再生手段によるコンテンツの再生に応じて更新する。更新後ライセンス情報生成手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えてコンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する。暗号化手段は、更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を利用者

が携帯するライセンス記憶装置の装置IDを用いて暗号化する。書き換え手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化手段によって暗号化された更新後ライセンス情報に書き換える。

【0030】上記コンテンツ再生装置では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0031】この発明のさらにもう1つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置ID、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置IDを暗号化して暗号化装置IDを生成する。復号手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、認証手段によって生成された暗号化装置IDを用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0032】この発明のさらにもう1つの局面に従うと、ライセンス発行方法は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。そして、ライセンス発行方法は、認証ステップと、書き込みステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。書き込みステップでは、利用者が携帯するライセンス記憶装置が正当なものであると認証ステップによって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【0033】上記ライセンス発行方法では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯

し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0034】また、ライセンス情報は、ライセンス記憶装置の装置IDを用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0035】また、上記ライセンス発行方法では、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【0036】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【0037】この発明のさらにもう1つの局面に従うと、コンテンツ再生方法は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生方法は、携帯可能なライセンス記憶装置の装置IDを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生方法は、認証ステップと、復号ステップと、再生ステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。復号ステップでは、認証ステップにおいて利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、当該利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置IDを用いて復号する。再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0038】上記コンテンツ再生方法では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツの提供を受けることができる。

【0039】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0040】好ましくは、上記再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【0041】上記コンテンツ再生方法では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無量大のコンテンツサーバを所有することと同様の効果が得られる。

【0042】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものである。そして、上記再生ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0043】好ましくは、上記コンテンツ再生方法はさらに、更新ステップと、暗号化ステップと、書き換えステップとを備える。更新ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、再生ステップにおけるコンテンツの再生に応じて更新する。暗号化ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に代えて更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化する。書き換えステップでは、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化ステップによって暗号化された更新後ライセンス情報に書き換える。

【0044】上記コンテンツ再生方法では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0045】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付し、その説明は繰り返さない。また、この発明では暗号アルゴリズムに制限を設けていないが、以下の実施の形態における説明では、特に断りのない限り暗号アルゴリズムとして暗号鍵と復号鍵に同一の鍵を用いる共通鍵暗号方式を想定している。

【0046】(第1の実施形態) 図1は、この発明の第1の実施形態によるコンテンツ提供システムの構成を示す図である。図1を参照して、このコンテンツ提供システムでは、ソフトウェア、音楽、映像などの電子的な著作物であるデジタルコンテンツ(以下、コンテンツという。)と、当該コンテンツの利用を許可するライセンス



情報とが分離して配布される。コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして配布される。また、暗号化コンテンツは、ネットワーク、放送、パッケージなどさまざまな形態で配布される。

【0047】コンテンツの提供を希望する利用者は、メモリカード100をライセンス発行装置200に挿入する。ライセンス発行装置200は、利用者が希望するコンテンツの利用を許可するライセンス情報を、利用者が携帯するメモリカード100の装置IDを用いて暗号化して、当該メモリカード100に書き込む。すなわち、メモリカード100には暗号化ライセンス情報だけが書き込まれる。そして利用者は、暗号化ライセンス情報が書き込まれたメモリカード100をコンテンツ再生装置300に挿入する。コンテンツ再生装置300は、利用者が携帯するメモリカード100に書き込まれたライセンス情報を、当該メモリカード100の装置IDを用いて復号する。そして、コンテンツ再生装置300は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。このようにして、コンテンツと、当該コンテンツの利用を許可するライセンス情報とが提供される。

【0048】以下、図1に示したメモリカード100、ライセンス発行装置200、およびコンテンツ再生装置300の具体的な構成、ライセンス発行装置200によるライセンス情報の発行の手順、ならびにコンテンツ再生装置300によるコンテンツの再生の手順について詳しく説明する。

【0049】図2は、図1に示したメモリカード100およびライセンス発行装置200の具体的な構成を示すブロック図である。以下、図2を参照しつつ説明する。

【0050】＜メモリカード100の構成＞メモリカード100は、携帯可能な独立したハードウェアであり、自己を一意に識別可能な装置IDを有する。そして、メモリカード100は、装置ID読み出し手段110と、相手装置認証手段120と、ライセンス記憶手段130とを備える。

【0051】装置ID読み出し手段110は、メモリカード100が有する装置IDを読み出して出力する。

【0052】相手装置認証手段120は、ライセンス情報を送受信する相手装置が正当な装置かどうかを認証する。相手装置は、ライセンス発行装置200からライセンス情報の提供を受ける場合にはライセンス発行装置200であり、コンテンツ再生装置300によってコンテンツの提供を受ける場合にはコンテンツ再生装置300である。相手装置認証手段120は、例えば、使用不可能なライセンス情報を発行してライセンス料のみを得るというような不正なライセンス発行装置を排除するために必要である。

【0053】ライセンス記憶手段130は、ライセンス

発行装置200からの暗号化されたライセンス情報を記憶する。ライセンス記憶手段130としては、例えば、フラッシュメモリなどが挙げられる。

【0054】＜ライセンス発行装置200の構成＞ライセンス発行装置200は、メモリカード認証手段210と、コンテンツID入力手段220と、コンテンツ利用条件入力手段230と、コンテンツ復号化鍵取得手段240と、連結手段250と、暗号化手段260とを備える。

【0055】メモリカード認証手段210は、メモリカード100が正当なものであるかどうかを認証する。メモリカード認証手段210は、認証に先立ってメモリカード100から装置IDを取得する。そしてメモリカード100との間で相互に認証を行った後、装置IDを暗号化して暗号化装置IDを出力する。これは、コンテンツを再生する際にコンテンツ再生装置300で同一の鍵を得るためである。

【0056】コンテンツID入力手段220は、利用者が指定したコンテンツに対するコンテンツIDを出力する。コンテンツIDとは、各コンテンツを識別するための記号である。コンテンツID入力手段220としては、例えば、キーボードやタッチパネルなどの入力装置によって利用者に直接に所望のコンテンツに対応したコンテンツIDの入力を促し、入力されたコンテンツIDをそのまま出力するものが挙げられる。また、別の例としては、ライセンス情報の発行が可能なコンテンツタイトルの一覧をディスプレイなどに表示して利用者に選択を促し、選択されたコンテンツタイトルに対するコンテンツIDを、図3に示すようなコンテンツタイトル31とコンテンツID32とが対応づけられたデータベースから取得するというものが挙げられる。なお、図3に示すデータベースでは、コンテンツタイトル31、コンテンツID32、およびコンテンツ復号化鍵33が対応づけられている。そして、コンテンツ復号化鍵33の情報は、外部から読み出すことができないように保護されている。

【0057】コンテンツ利用条件入力手段230は、コンテンツ利用条件を出力する。コンテンツ利用条件とは、コンテンツを利用する際の制限事項を示す情報である。コンテンツ利用条件としては、例えば、コンテンツがソフトウェアプログラムである場合に、「扱うデータ量は100Kバイトまでとする」というような制限事項を示す情報が挙げられる。また、別の例としては、コンテンツが音楽データの場合に、「再生することができる期間」を示す情報が挙げられる。コンテンツ利用条件はコンテンツの特性に応じてさまざまなものが考えられるため、コンテンツまたはコンテンツのカテゴリに対応した利用条件データベースを設けてもよい。この場合にも、上述したコンテンツID入力手段220におけるのと同様に、利用者に利用条件の一覧を提示して利用者に

選択を促すなどの方法がある。

【0058】コンテンツ復号化鍵取得手段240は、コンテンツID入力手段220からのコンテンツIDを受け、当該コンテンツIDに対応するコンテンツを暗号化された状態から復号するための鍵を取得する。例えば、図3に示したデータベースを参照して取得することができる。

【0059】連結手段250は、コンテンツID入力手段220からのコンテンツID、コンテンツ利用条件入力手段230からのコンテンツ利用条件、およびコンテンツ復号化鍵取得手段240からのコンテンツ復号化鍵を連結してライセンス情報を生成する。

【0060】暗号化手段260は、連結手段250によって生成されたライセンス情報をメモ리카ード認証手段210からの暗号化装置IDで暗号化して暗号化ライセンス情報を生成する。そして、暗号化手段260は、暗号化ライセンス情報をメモ리카ード100のライセンス記憶手段130へ書き込む。

【0061】＜ライセンス情報の発行の手順＞図4は、図2に示したライセンス発行装置200によるライセンス情報の発行の手順を示すフローチャートである。以下、図4および図2を参照しつつライセンス情報の発行の手順について説明する。

【0062】まず、ステップST401において、利用者は、メモ리카ード100をライセンス発行装置200の所定の挿入口に差し込む。これにより、メモ리카ード100に設けられたピンとライセンス発行装置200のソケットとの間が電氣的に接続される。この結果、メモ리카ード100とライセンス発行装置200との間で、お互いにデータを送受信するための通信手段が確保される。

【0063】次いで、ステップST402において、メモ리카ード100とライセンス発行装置200との間で、お互いが正当な装置であることの認証が行われる。この相互認証の手順については後述する。相互認証中にエラーが発生した場合には処理が中断されて利用者にその旨が知らされる。相互認証を行った後、メモ리카ード認証手段210は、メモ리카ード100の装置IDを暗号化して暗号化装置IDを生成する。

【0064】次いで、ステップST403において、利用者は、コンテンツID入力手段220を利用して、希望するコンテンツに対応するコンテンツIDを入力する。これにより、利用者が希望するコンテンツに対応するコンテンツIDが得られる。

【0065】次いで、ステップST404において、利用者は、コンテンツ利用条件入力手段230を利用して、コンテンツ利用条件を入力する。これにより、利用者が希望するコンテンツに対するコンテンツ利用条件が得られる。

【0066】次いで、ステップST405において、利

用者は、希望するコンテンツおよびその利用条件に対応した料金を支払う。料金の支払い手段/方法としては、種々の公知の手段/方法を利用することができる。

【0067】次いで、ステップST406において、コンテンツ復号化鍵取得手段240は、ステップST403において得られたコンテンツIDに対応するコンテンツを暗号化された状態から復号するための鍵を取得する。ここでは、図3に示したデータベースを参照して取得する。

【0068】次いで、ステップST407において、連結手段250は、ステップST403において得られたコンテンツID、ステップST404において得られたコンテンツ利用条件、およびステップST406において得られたコンテンツ復号化鍵を連結してライセンス情報を生成する。

【0069】次いで、ステップST408において、暗号化手段260は、ステップST407において得られたライセンス情報をステップST402において得られた暗号化装置IDで暗号化して暗号化ライセンス情報を生成する。

【0070】次いで、ステップST409において、暗号化手段260は、ステップST408において得られた暗号化ライセンス情報をメモ리카ード100のライセンス記憶手段130へ書き込む。通常、メモ리카ード100のライセンス記憶手段130には、複数のコンテンツの暗号化ライセンス情報が記憶される。そこで、ライセンス記憶手段130に暗号化ライセンス情報を書き込む際には、図5に示すように、暗号化ライセンス情報53に対応づけてコンテンツタイトル51、コンテンツ付属情報52なども書き込んでおく。これにより、後で利用者が、複数の暗号化ライセンス情報から希望のコンテンツを指示することが容易となる。

【0071】このようにして、利用者の希望するコンテンツのライセンス情報が、利用者の携帯するメモ리카ード100のライセンス記憶手段130に書き込まれる。

【0072】以上のように、第1の実施形態におけるライセンス発行装置200は、メモ리카ード認証手段210と、暗号化手段260とを設けたため、コンテンツと分離したライセンス情報を、正当と認識されたメモ리카ード100へ記憶させることができる。

【0073】また、利用者が希望するコンテンツ自体は書き込まずにそのコンテンツのライセンス情報だけを、利用者の携帯するメモ리카ード100に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、メモ리카ード100のライセンス記憶手段130の記憶容量を気にする必要もない。

【0074】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのメ

メモリカード100でたくさんのコンテンツを利用することができる。

【0075】なお、ここでは、連結手段250によって生成されるライセンス情報にはコンテンツ利用条件が含まれているが、コンテンツ利用条件を用いずにコンテンツIDとコンテンツ復号化鍵とを連結してライセンス情報を生成してもよい。この場合は、コンテンツ利用条件入力手段230を設ける必要はない。

【0076】また、コンテンツ復号化鍵を用いずにコンテンツIDとコンテンツ利用条件とを連結してライセンス情報を生成してもよい。この場合、ライセンス発行装置200にコンテンツ復号化鍵取得手段240を設ける必要はなくなるが、その代わりに、コンテンツ再生装置300にコンテンツ復号化鍵取得手段を設ける必要がある。

【0077】＜相互認証の手順＞次に、図4に示したステップST402における相互認証の手順について、図6および図2を参照しつつ説明する。なお、図6中、ステップST601-ST606はメモリカード100の相手装置認証手段120における処理、ステップST611-ST616はライセンス発行装置200のメモリカード認証手段210における処理を示す。

【0078】認証に先立って、ライセンス発行装置200のメモリカード認証手段210は、メモリカード100から装置ID(i d)を取得する。このように、メモリカード100およびライセンス発行装置200は、あらかじめメモリカード100の装置ID(i d)を共有しておく。さらに、メモリカード100は装置鍵K d1を、ライセンス発行装置200は装置鍵K d2を持つ。装置鍵K d1、K d2は、それぞれの装置自身で保持し、外部から読み出しできないようにしておく。望ましくは、解析できないような耐タンパー装置で防御されている。メモリカード100およびライセンス発行装置200がお互いに正当な装置であれば、装置鍵K d1と装置鍵K d2は同一であるものとする。

【0079】まず、ステップST601において、メモリカード100の相手装置認証手段120は、暗号化装置ID(E i 1)を生成する。暗号化装置ID(E i 1)は、メモリカード100の装置ID(i d)を装置鍵K d1を用いて暗号化することによって生成される。これを図6では、 $E i 1 = F(K d 1, i d)$ と表している。

【0080】一方、ステップST611において、ライセンス発行装置200のメモリカード認証手段210は、暗号化装置ID(E i 2)を生成する。暗号化装置ID(E i 2)は、メモリカード100の装置ID(i d)を装置鍵K d2を用いて暗号化することによって生成される。これを図6では、 $E i 2 = F(K d 2, i d)$ と表している。

【0081】そして以下の処理によって、お互いが有す

る暗号化装置ID(E i 1, E i 2)が同一であることを、暗号化装置ID(E i 1, E i 2)を装置外部の通信手段を用いてやりとりすることなく確認することによって、お互いの装置の正当性を認証する。

【0082】ステップST602において、メモリカード100の相手装置認証手段120は、乱数R1を生成し、ライセンス発行装置200のメモリカード認証手段210へ送信する。

【0083】そして、ステップST603において、メモリカード100の相手装置認証手段120は、乱数R1を暗号化装置ID(E i 1)を用いて暗号化して暗号化乱数E1 r1を生成する。これを図6では、 $E1 r1 = E(E i 1, R1)$ と表している。

【0084】一方、ステップST612において、ライセンス発行装置200のメモリカード認証手段210は、受信した乱数R1を暗号化装置ID(E i 2)を用いて暗号化して暗号化乱数E2 r1を生成する。これを図6では、 $E2 r1 = E(E i 2, R1)$ と表している。そして、ライセンス発行装置200のメモリカード認証手段210は、暗号化乱数E2 r1をメモリカード100の相手装置認証手段120へ送信する。

【0085】次いで、ステップST604において、メモリカード100の相手装置認証手段120は、ステップST603において生成した暗号化乱数E1 r1と、ステップST612において受信した暗号化乱数E2 r1とを比較する。比較の結果、両者が一致しないときは、ステップST606に進み、相手装置認証手段120は、ライセンス発行装置200が正当なものではないとみなし(エラー発生)、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、相手装置認証手段120は、ライセンス発行装置200が正当なものであるとみなし、ステップST605に進む。

【0086】ステップST613において、ライセンス発行装置200のメモリカード認証手段210は、乱数R2を生成し、メモリカード100の相手装置認証手段120へ送信する。

【0087】そして、ステップST614において、ライセンス発行装置200のメモリカード認証手段210は、乱数R2を暗号化装置ID(E i 2)を用いて暗号化して暗号化乱数E2 r2を生成する。これを図6では、 $E2 r2 = E(E i 2, R2)$ と表している。

【0088】一方、ステップST605において、メモリカード100の相手装置認証手段120は、受信した乱数R2を暗号化装置ID(E i 1)を用いて暗号化して暗号化乱数E1 r2を生成する。これを図6では、 $E1 r2 = E(E i 1, R2)$ と表している。そして、メモリカード100の相手装置認証手段120は、暗号化乱数E1 r2をライセンス発行装置200のメモリカード認証手段210へ送信する。

【0089】次いで、ステップST615において、ライセンス発行装置200のメモリカード認証手段210は、ステップST614において生成した暗号化乱数E2r2と、ステップST605において受信した暗号化乱数E1r2とを比較する。比較の結果、両者が一致しないときは、ステップST616に進み、ライセンス発行装置200のメモリカード認証手段210は、メモリカード100が正当なものではないとみなし（エラー発生）、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、ライセンス発行装置200のメモリカード認証手段210は、メモリカード100が正当なものであるとみなす。

【0090】以上のようにして、メモリカード100とライセンス発行装置200との間で、お互いが正当な装置であることの認証（相互認証）が行われる。

【0091】そして、相互認証の手続きが終了した後、メモリカード認証手段210は、暗号化装置ID（Ei2）を暗号化手段260へ出力する。

【0092】なお、ここでは装置鍵Kd1、Kd2を用いているが、これらを用いず、装置IDに特定の変換Fを施してEi1、Ei2を得ることもできる。この場合は、変換Fを非公開にして、変換方法が共通である装置を正当な装置を認証することとなる。

【0093】＜コンテンツ再生装置300の構成＞図7は、図1に示したメモリカード100およびコンテンツ再生装置300の具体的な構成を示すブロック図である。以下、図7を参照してコンテンツ再生装置300の具体的な構成について説明する。

【0094】コンテンツ再生装置300は、メモリカード認証手段210と、コンテンツID入力手段220と、復号手段310と、分離手段320と、比較手段330と、再生手段340と、暗号化コンテンツデータベース350とを備える。

【0095】復号手段310は、メモリカード100のライセンス記憶手段130に記憶された暗号化ライセンス情報を読み出し、読み出した暗号化ライセンス情報をメモリカード認証手段210からの暗号化装置IDを用いて復号してライセンス情報を得る。

【0096】分離手段320は、復号手段310によって得られたライセンス情報から、コンテンツID、コンテンツ利用条件、およびコンテンツ復号化鍵を得る。

【0097】比較手段330は、分離手段によって得られたコンテンツIDとコンテンツID入力手段220によって得られたコンテンツIDとを比較し、両者が一致するときは、再生指示信号を再生手段340に出力する。

【0098】暗号化コンテンツデータベース350には、コンテンツをそのままでは利用できないように暗号化した暗号化コンテンツが格納されている。

【0099】再生手段340は、比較手段330からの

再生指示信号にตอบสนองして、分離手段320によって得られたコンテンツIDに対応する暗号化コンテンツを暗号化コンテンツデータベース350から取得する。そして再生手段340は、取得した暗号化コンテンツを分離手段320によって得られたコンテンツ復号化鍵を用いて復号し、分離手段320によって得られたコンテンツ利用条件に従って再生する。

【0100】＜コンテンツの再生の手順＞図8は、図7に示したコンテンツ再生装置300によるコンテンツの再生の手順を示すフローチャートである。以下、図8および図7を参照しつつコンテンツの再生の手順について説明する。

【0101】まず、ステップST801において、利用者は、再生を希望するコンテンツに対する暗号化ライセンス情報が記憶されたメモリカード100をコンテンツ再生装置300の所定の挿入口に差し込む。これにより、メモリカード100に設けられたピンとコンテンツ再生装置300のソケットとの間が電氣的に接続される。この結果、メモリカード100とコンテンツ再生装置300との間で、お互いにデータを送受信するための通信手段が確保される。

【0102】次いで、ステップST802において、メモリカード100とコンテンツ再生装置300との間で、お互いが正当な装置であることの認証が行われる。この相互認証は、図6に示したのと同様の手順で行われる。相互認証を行った後、コンテンツ再生装置300のメモリカード認証手段210は、メモリカード100の装置IDを暗号化して暗号化装置IDを生成する。

【0103】次いで、ステップST803において、利用者は、コンテンツID入力手段220を利用して、再生を希望するコンテンツに対するコンテンツIDを入力する。通常、メモリカード100のライセンス記憶手段130には、複数の暗号化ライセンス情報が記憶されている。しかし、図5に示したように、メモリカード100のライセンス記憶手段130には、暗号化ライセンス情報53に対応づけてコンテンツタイトル51、コンテンツ付属情報52なども記憶されている。したがって、メモリカード100のライセンス記憶手段130に記憶されているコンテンツタイトル／コンテンツ付属情報の一覧を利用者に提示して、希望するコンテンツタイトルを選択させた後、図3に示したのと同様のデータベースを用いてコンテンツIDを得ることができる。

【0104】次いで、ステップST804において、復号手段310は、メモリカード100のライセンス記憶手段130から、利用者が再生を希望するコンテンツに対する暗号化ライセンス情報を読み出す。ここでは、ステップST803において利用者が選択したコンテンツタイトルを用いることによって、復号すべき暗号化ライセンス情報を容易に特定することができる。そして、復号手段310は、読み出した暗号化ライセンス情報を、

ステップST802においてメモリカード認証手段210によって生成された暗号化装置IDを用いて復号し、ライセンス情報を得る。

【0105】次いで、ステップST805において、分離手段330は、復号手段310によって得られたライセンス情報を、コンテンツID、コンテンツ復号化鍵、およびコンテンツ利用条件に分離する。

【0106】次いで、ステップST806において、比較手段330は、ステップST803においてコンテンツID入力手段220によって得られたコンテンツIDと、ステップST805において分離手段320によって得られたコンテンツIDとを比較する。比較の結果、両者が同一であれば、このライセンス情報は正当なライセンス発行装置によって発行されたものであるとみなし、比較手段330は、再生指示信号を再生手段340に出力する。

【0107】次いで、ステップST807において、再生手段340は、比較手段330からの再生指示信号に応答して、分離手段320によって得られたコンテンツIDに対応する暗号化コンテンツを暗号化コンテンツデータベース350から取得する。そして再生手段340は、取得した暗号化コンテンツを分離手段320によって得られたコンテンツ復号化鍵を用いて復号し、分離手段320によって得られたコンテンツ利用条件に従って再生する。例えば、コンテンツ利用条件として利用可能な期限が付加されたものであれば、現在の日付と利用可能な期限とを比較することにより、再生を行うかどうかを再生前に判断する。

【0108】このようにして、利用者が希望するコンテンツの再生が行われる。

【0109】以上のように、第1の実施形態におけるコンテンツ再生装置300は、メモリカード認証手段210と、復号手段310と、再生手段340とを設けたため、コンテンツと分離したライセンス情報を、正当と認識されたメモリカード100から読み込んで、対応するコンテンツを再生することができる。

【0110】なお、ここでは、暗号化コンテンツデータベース350をコンテンツ再生装置300内に設けたが、これを外部、例えば、通信回線を介して遠隔地に設けてもよい。この場合、コンテンツ再生装置300は、コンテンツIDのような情報でコンテンツを特定して、外部にある暗号化コンテンツデータベースより暗号化コンテンツを受信し、再生する。このように暗号化コンテンツデータベースを外部に設けることは、コンテンツ再生装置が大きな記憶容量を確保できない携帯端末である場合に有利である。

【0111】また、メモリカード100のライセンス記憶手段130に記憶されたライセンス情報にコンテンツ利用条件が含まれていない場合には、分離手段320ではコンテンツ利用条件は得られない。したがって、コン

テンツ再生手段340は利用条件を考慮する必要はない。

【0112】また、メモリカード100のライセンス記憶手段130に記憶されたライセンス情報にコンテンツ復号化鍵が含まれていない場合には、図5に示したようなコンテンツIDとコンテンツ復号化鍵とを対応づけたデータベースを設けておき、このデータベースを用いて、分離手段320によって得られたコンテンツIDよりコンテンツ復号化鍵を得ることができる。

【0113】また、メモリカード100のライセンス記憶手段130から読み込んだ暗号化ライセンス情報が十分信頼できるものである場合には、コンテンツID入力手段220および比較手段330を取り除いた構成とすることも可能である。

【0114】また、図2に示したライセンス発行装置200の暗号化手段260および図7に示したコンテンツ再生装置300の復号化手段310では、暗号/復号の鍵としてメモリカード認証手段210からの暗号化装置IDを用いているが、これに代えて、外部から読み出し不可能な非公開の鍵をライセンス発行装置200およびコンテンツ再生装置300にあらかじめ記憶させておき、これを暗号/復号の鍵としてもよい。さらにこの場合、暗号化/復号化の暗号アルゴリズムとして、例えばRSAのような非対称暗号を用い、それぞれの装置で対応する鍵を記憶しておくこともできる。

【0115】＜効果＞以上のように、この発明の第1の実施形態によるコンテンツ提供システムでは、ライセンス発行装置200は、コンテンツのライセンス情報を、携帯可能な独立したハードウェアであるメモリカード100に書き込む。そして、コンテンツ再生装置300は、メモリカード100に記憶されたライセンス情報に従ってコンテンツを再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたメモリカード100を携帯し、ライセンス発行装置200に対応したさまざまな形態のコンテンツ再生装置300を利用してコンテンツの提供を受けることができる。すなわち、利用者は、コンテンツ再生装置300の形態に制限されることなく、購入したコンテンツを利用することができる。

【0116】また、ライセンス情報は、暗号化装置IDを用いて暗号化/復号化される。すなわち、ライセンス情報は、個々のメモリカード100を一意に識別可能な装置IDを用いて暗号化/復号化される。これにより、暗号化ライセンス情報を不正にコピーしたメモリカードを用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0117】また、ライセンス発行装置200はコンテンツのライセンス情報だけを、利用者の携帯するメモリカード100に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセ

ンス情報の発行にかかる時間を増大させることがなく、また、メモリカード100のライセンス記憶手段130の記憶容量を気にする必要もない。

【0118】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのメモリカード100でたくさんのコンテンツを利用することができる。

【0119】また、コンテンツは暗号化されて配布され、ライセンス情報を購入しなければ再生が不可能なため、ネットワーク、放送、パッケージなど形態を問わず自由に流通させることが可能となり、かつ、利用者にとっては入手が容易となる。これにより、利用者は必ずしもコンテンツを所有する必要がなく、ライセンス情報のみを購入、携帯し、必要に応じてコンテンツにアクセスすればよい。この結果、利用者側でコンテンツを蓄積するための大容量のデータ蓄積装置を確保できない場合は、コンテンツの再生時にその都度ダウンロードすることによって、仮想的に容量が無量大のコンテンツサーバを所有することと同様の効果が得られる。一方、利用者側に大容量のデータ蓄積装置を確保できる場合は、事前に再生する可能性のあるコンテンツをすべてダウンロードしておき、再生時にはライセンス情報を購入することによって、ダウンロードに時間のかかる大容量のコンテンツを即座に再生することが可能となる。

【0120】(第2の実施形態)この発明の第2の実施形態によるコンテンツ提供システムでは、図7に示したコンテンツ再生システム300に代えて、図9に示すコンテンツ再生装置900を備える。そして、その他の構成を第1の実施形態におけるコンテンツ提供システムと同じくする。

【0121】<コンテンツ再生装置900の構成>図9を参照して、このコンテンツ再生装置900は、メモリカード認証手段210と、コンテンツID入力手段220と、復号手段310と、分離手段320と、比較手段330と、再生手段340と、暗号化コンテンツデータベース350と、コンテンツ利用条件更新手段910と、連結手段920と、暗号化手段930と、暗号化ライセンス情報更新手段940とを備える。

【0122】再生手段340は、第1の実施形態において説明した動作に加えてさらに、コンテンツを再生したことを示す再生検知信号を生成し、コンテンツ利用条件を出力する。

【0123】コンテンツ利用条件更新手段910は、コンテンツ再生手段340からの再生検知信号を受けて、コンテンツ再生手段340からコンテンツ利用条件を読み込み、当該コンテンツ利用条件を更新して更新後コンテンツ利用条件を生成する。これは、コンテンツの再生前後でコンテンツ利用条件が変化する場合(例えば、コンテンツ利用条件として「コンテンツを利用することができる回数」が定められている場合など)を想定してい

る。このように利用回数に制限が存在する場合は、1回再生するごとに残りの利用回数を減じていかなければならない。そして減じた後の利用回数を新たにコンテンツの利用条件として更新することが必要となる。

【0124】連結手段920は、コンテンツ利用条件更新手段910からの更新後コンテンツ利用条件と、分離手段320からのコンテンツIDおよびコンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【0125】暗号化手段930は、連結手段920からの更新後ライセンス情報をメモリカード認証手段210からの暗号化装置IDを用いて暗号化して、更新後暗号化ライセンス情報を生成する。

【0126】暗号化ライセンス情報更新手段940は、メモリカード100のライセンス記憶手段130に記憶されている暗号化ライセンス情報を、暗号化手段930によって生成された更新後暗号化ライセンス情報に書き換える。

【0127】<コンテンツ再生装置900の動作>以下、図9に示したコンテンツ再生装置900の動作について説明する。

【0128】コンテンツ再生装置900は、図8に示したステップST801-ST807における処理と同様の処理によってコンテンツの再生を行う。

【0129】そして、コンテンツの再生が終了した後またはコンテンツの再生中に、再生手段340は、再生検知信号をコンテンツ利用条件更新手段910に出力する。

【0130】次いで、コンテンツ利用条件更新手段910は、再生検知信号を受けて、再生手段340からコンテンツ利用条件を読み込み、当該コンテンツ利用条件のうち再生に応じて変更すべき部分を変更する。例えば、コンテンツ利用条件が「再生可能な回数は3である」という条件であれば、再生可能な回数を1減じて2と変更する。そして、これを更新後コンテンツ利用条件として連結手段920へ出力する。

【0131】次いで、連結手段920は、更新後コンテンツ利用条件と、コンテンツIDと、コンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【0132】次いで、暗号化手段930は、更新後ライセンス情報を暗号化装置IDを用いて暗号化する。

【0133】次いで、暗号化ライセンス情報更新手段940は、メモリカード100のライセンス記憶手段130に記憶されている暗号化ライセンス情報を消去し、更新後暗号化ライセンス情報を書き込む。

【0134】<効果>以上のように、第2の実施形態によるコンテンツ再生装置900は、コンテンツ利用条件更新手段910と、連結手段920と、暗号化手段930と、暗号化ライセンス情報更新手段940とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新すること

ができ、正しいコンテンツ利用条件を保持することが可能となる。

【0135】(第3の実施形態)図10は、図1に示したコンテンツ提供システムの適用例を示す図である。以下、図10を参照して、コンテンツ提供システムの適用例について説明する。

【0136】ライセンス発行装置200は、駅、コンビニ、店頭などに設置されたり(200a)、パソコンや携帯電話などの端末400から有線、無線を問わずアクセス可能なネットワークに接続されたりする(200b)。そして、利用者は、ライセンス発行装置200aまたは端末400にメモリカード100を挿入し、ガイドランスに従って希望のコンテンツ(音楽、映画、ゲーム、電子本など)を選択して、表示された料金を支払う。ライセンス発行装置200a、200bは、利用者が選択したコンテンツに対するライセンス情報を、メモリカード100の装置IDを用いて暗号化してメモリカード100へ書き込む。書き込みが終了すると、利用者はレシートを受け取り、メモリカード100を取り出す。このように、利用者は、自宅/外出先のいずれにおいても、希望するコンテンツの暗号化ライセンス情報をメモリカード100に書き込むことができる。そして、利用者は、CDやMDなどの希望のコンテンツが格納された媒体を持ち歩く必要はなく、ライセンス情報だけが書き込まれたメモリカード100を携帯すればよい。

【0137】一方、コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして、ネットワーク、放送、パッケージなどのさまざまな形態で流通している。

【0138】そして、利用者の自宅に設けられたホームサーバ350aには、パソコンからネットワーク経由でダウンロードした暗号化コンテンツや、デジタルTVのデータ放送を受信して得られた暗号化コンテンツなどが蓄積されている。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードを自宅にあるコンテンツ再生装置300aに挿入することによって、コンテンツの提供を受けることができる。

【0139】また、外出先(列車、飛行機などの交通機関、自動車、店、図書館、ホテルなど)にも、コンテンツサーバ350b、コンテンツ再生装置300bが設けられている。コンテンツ再生装置300bは、コンテンツの提供者側が用意するものであってもよいし、利用者が所持する携帯端末を利用してもよい。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードをコンテンツ再生装置300bに挿入することによって、コンテンツの提供を受けることができる。

【0140】コンテンツ提供者にとっては、豊富なコンテンツを提供することによる集客効果、差別化、徴収した利用料などのメリットが得られる。また、コンテンツ

の再生中にCMを流して広告収入を得たり、自店舗の紹介をしたりすることができる。さらに、高音質、高画質を売りにしたコンテンツ再生装置を用意して、その利用料を徴収することもできる(例えば、ハイビジョン映像なら100円増しにするなど)。

【0141】利用者にとっては、好きな音楽を、自宅、車の中、電車の中、船の中、飛行機の中などで聴くことができる。しかも、CDやMDなどの媒体や再生装置を持ち歩く必要がなく、メモリカード1枚だけでよい。

【0142】また、利用者は、最近はやりの個室スペースで、音楽を聴いたり、映画を見たり、本を読んだり、ゲームをしたりというようにさまざまなコンテンツを提供を受けることができる。この場合、個室スペースの提供者は、メモリカードにライセンス情報が書き込まれていれば個室スペースの利用料を無料とすることもできる。ライセンス発行装置が設けられていれば、利用者は、メモリカードにライセンス情報が書き込まれていない場合にも、その場で購入することができる。

【0143】また、利用者は、旅行先で見所を調べるために、旅行前に買った雑誌(コンテンツ)へアクセスして調べることもできる。これにより、利用者は、雑誌、新聞、百科事典などを持ち歩く必要がなくなる。

【0144】

【発明の効果】この発明の1つの局面に従ったライセンス発行装置は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0145】また、ライセンス情報は、ライセンス記憶装置の装置IDを用いて暗号化されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0146】また、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込むため、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【0147】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【0148】また、ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続されるため、利用者はライセンス発行装置と距離的に離れた所においても、ネットワークを介してライセンス発行

装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【0149】この発明のもう1つの局面に従ったコンテンツ再生装置は、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0150】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0151】また、蓄積手段を設けたため、再生する可能性のあるコンテンツをあらかじめすべて蓄積しておくことができる。これにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【0152】また、再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得するため、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得することができる。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0153】また、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0154】この発明のさらにもう1つの局面に従ったライセンス発行方法は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0155】この発明のさらにもう1つの局面に従ったコンテンツ再生方法は、利用者が携帯するライセンス記

憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツの提供を受けることができる。

【図面の簡単な説明】

【図1】この発明の第1の実施形態によるコンテンツ提供システムの構成を示す図である。

【図2】図1に示したメモリカードおよびライセンス発行装置の具体的な構成を示すブロック図である。

【図3】コンテンツタイトル、コンテンツID、およびコンテンツ復号化鍵が対応づけられたデータベースのデータ構造を示す図である。

【図4】図2に示したライセンス発行装置によるライセンス情報の発行の手順を示すフローチャートである。

【図5】メモリカードのライセンス記憶手段に記憶される情報を示す図である。

【図6】メモリカードとライセンス発行装置との間での相互認証の手順を示すフローチャートである。

【図7】図1に示したメモリカードおよびコンテンツ再生装置の具体的な構成を示すブロック図である。

【図8】図7に示したコンテンツ再生装置によるコンテンツの再生の手順を示すフローチャートである。

【図9】この発明の第2の実施形態によるコンテンツ再生装置の構成を示すブロック図である。

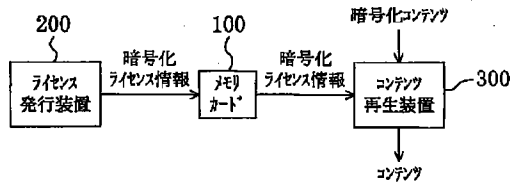
【図10】図1に示したコンテンツ提供システムの適用例を示す図である。

【符号の説明】

- 100   メモリカード
- 120   相手装置認証手段
- 130   ライセンス記憶手段
- 200, 200a, 200b   ライセンス発行装置
- 210   メモリカード認証手段
- 250, 920   連結手段
- 260, 930   暗号化手段
- 300, 900, 300a, 300b   コンテンツ再生装置
- 310   復号手段
- 340   再生手段
- 350, 350a, 350b   暗号化コンテンツデータベース
- 910   コンテンツ利用条件更新手段
- 940   暗号化ライセンス情報更新手段



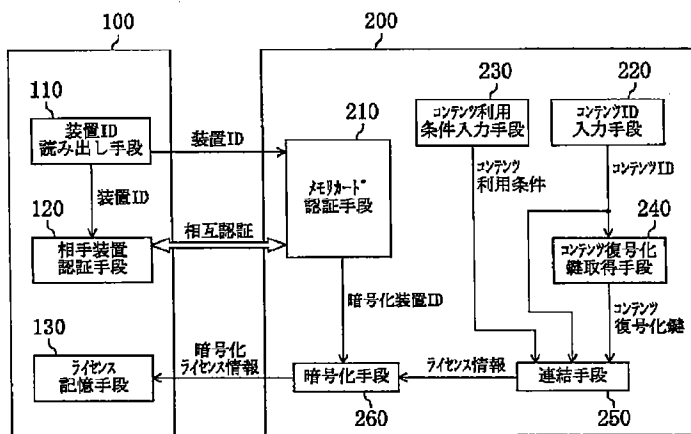
【図1】



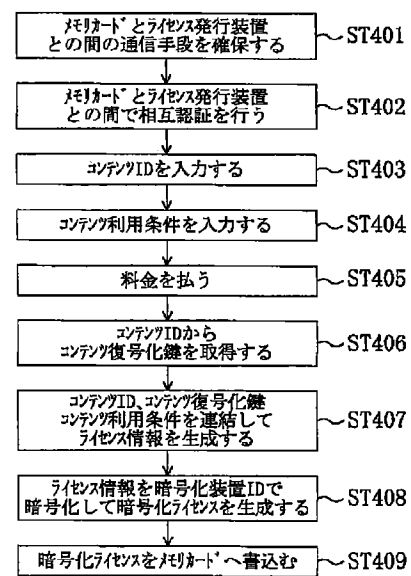
【図3】

31	32	33
音楽1	0001	SSSS1
音楽2	0002	TTTT2
映画1	0003	UUUU3
映画2	0004	VVVV4
⋮	⋮	⋮

【図2】



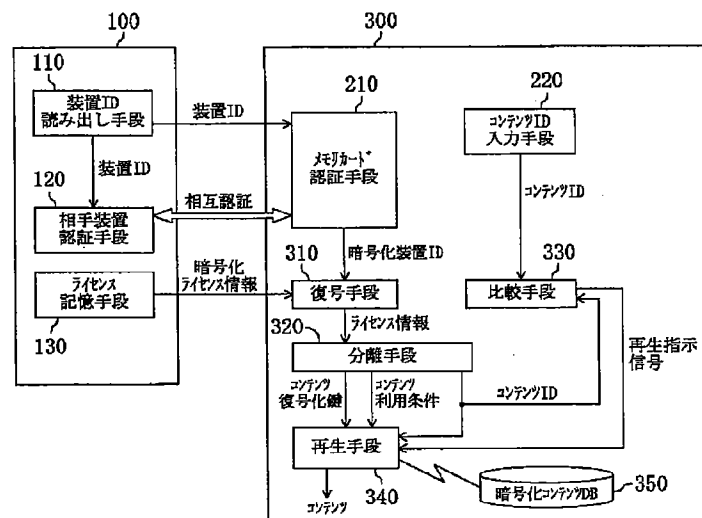
【図4】



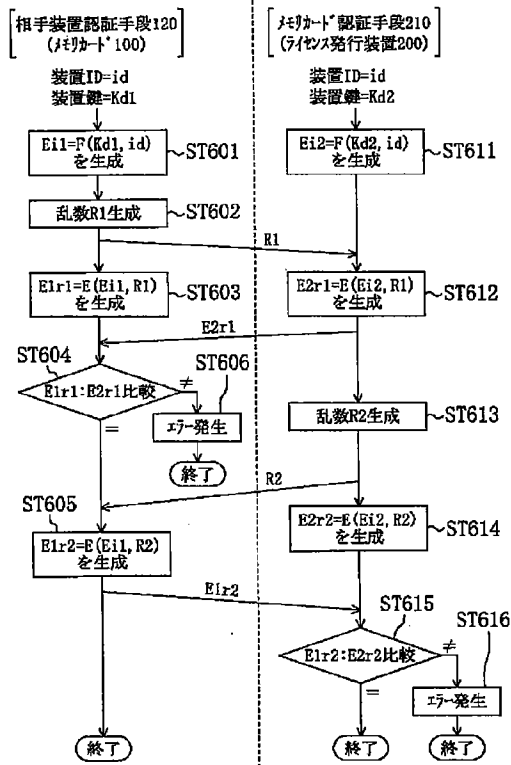
【図5】

51	52	53
音楽A	歌手1	XXABCD
音楽B	歌手2	XXEFGH
映画A	俳優1	XXJKLM
⋮	⋮	⋮

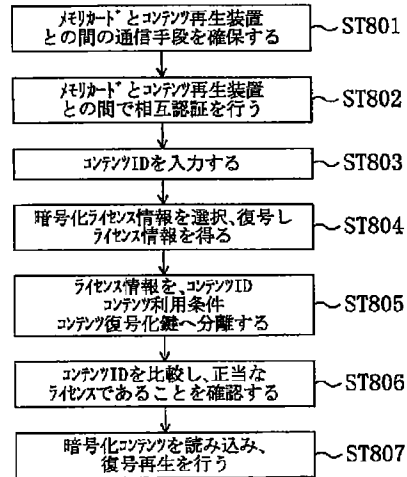
【図7】



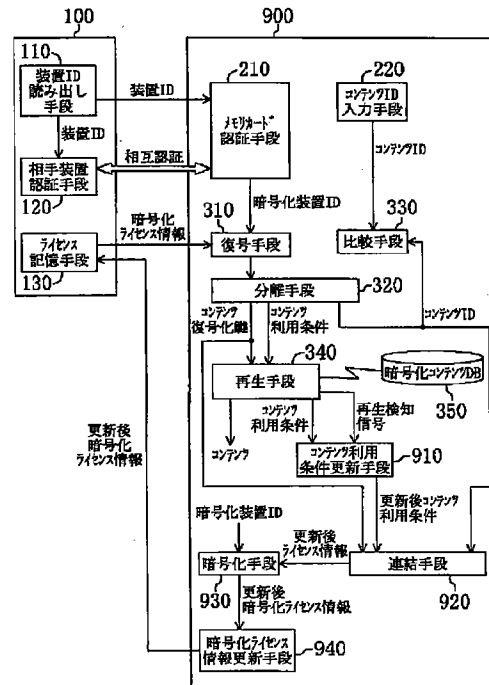
【図6】



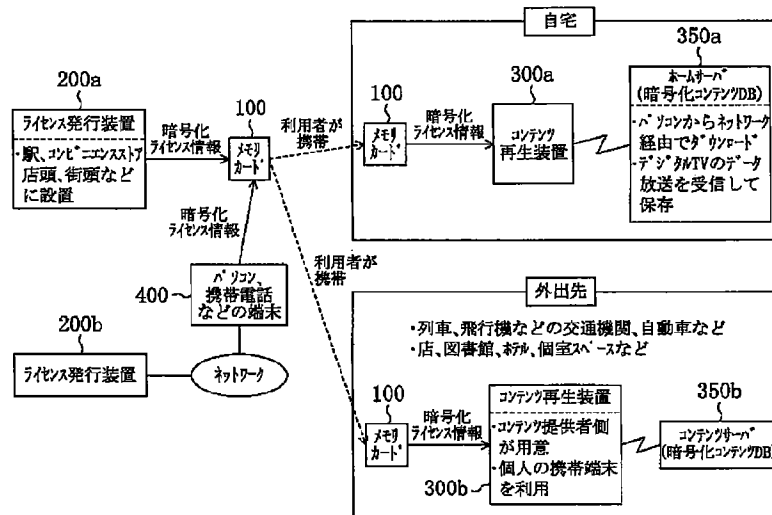
【図8】



【図9】



【図10】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

G 0 6 F 17/60

H 0 4 L 9/08

9/32

識別記号

3 0 2

F I

G 0 6 F 9/06

H 0 4 L 9/00

ノート (参考)

6 6 0 F

6 0 1 A

6 7 3 B